TRAI

Consultation Paper
On
Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services

TRAI Questions & Verimatrix Responses

Verimatrix
Impasse des Carrés de l'Arc
Rond-point du Canet
13590, Meyreuil
France

Table of Contents

Overview

About This Document

The Indian government is currently seeking support from the players in the broadcast market in India to ensure that conditional access systems (CAS) and subscriber management systems (SMS) in the broadcasting and cable industries are technically compliant with local regulations.

Verimatrix is a vendor offering highly secure CA solutions for both one-way and two-way networks.

This document describes Verimatrix' view and recommendations regarding the compliance of such CAS and SMS solutions.

TRAI Questions and Verimatrix Responses

Q1: List all the important features of CAS & SMS to adequately cover all the requirements for Digital Addressable Systems with a focus on the content protection and the factual reporting of subscriptions. Please provide exhaustive list, including the features specified in Schedule III of Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017?

Verimatrix is a CAS vendor. Hence this answer is limited to the CAS part. Typical features a CAS should support are listed in the following:

- Advanced/Ultra security with support by trusted hardware (TEE or IPR)
- Studio certification
- Individual ECM encryption
- Proprietary key ladders
- STB blacklisting features
- Entitlements expire without a need de-entitlement
- Individual and group based EMM addressing
- Simulcrypt compliance
- Fingerprinting and forensic watermarking
- OSM messaging
- Triggers
- Reporting capabilities to allow for reconciliation of the data residing in the CAS data base.

Q2: As per audit procedure (in compliance with Schedule III), a certificate from CAS / SMS vendor suffices to confirm the compliance. Do you think that all the CAS & SMS comply with the requisite features as enumerated in question 1 above? If not, what additional checks or compliance measures are required to improve the compliance of CAS/SMS?

Vendors should commit compliance by self-declaration.

Q3: Do you consider that there is a need to define a framework for CAS/ SMS systems to benchmark the minimum requirements of the system before these can be deployed by any DPO in India?

If Q1 is met by a known and well-established CAS vendor, then self-declaration should be sufficient. For other vendors or newcomers, meeting high security is must. There should be a framework to ensure that new vendors approaching the market in India are compliant.

Q4: What safeguards are necessary so that consumers as well as other stakeholders do not suffer for want of regular upgrade/ configuration by CAS/ SMS vendors?

CA systems shall be maintained with latest updates from the CAS vendor to ensure reliable platform security and that system outages and content leaks are avoided.

Q5.a: Who should be entrusted with the task of defining the framework for CAS & SMS in India? Justify your choice with reasons thereof. Describe the structure and functioning procedure of such entrusted entity.

Any TRAI nominated body should be good to define the framework, Verimatrix is neutral to it. Verimatrix will provide full support to that body.

Q5.b: What should be the mechanism / structure, so as to ensure that stakeholders engage actively in the decision-making process for making test specifications / procedures? Support your response with any existing model adapted in India or globally.

This should be defined by the TRAI nominated body (see Q5.a)

Q6: Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism.

It depends a lot on the targeted solution. For example, Common Interface Modules are directly available. The ETSI ECI proposal needs further investigation, also to which extent it can meet typical content provider and CAS security requirements.

Q6.a: Should there be a designated agency to carry out the testing and certification to ensure compliance to such framework? Or alternatively should the work of testing and certification be entrusted with accredited testing labs empanelled by the standards making agency / government? Please provide detailed suggestion including the benefits and limitations (if any) of the suggested model.

Operator and CAS vendor shall continue to work together. TRAI nominated body should only involve if there is any non-compliance by either party.

Q6.b: What precaution should be taken at the planning stage for smooth implementation of standardization and certification of CAS and SMS in Indian market? Do you foresee any challenges in implementation?

Operator and CAS vendor shall continue to work together. TRAI nominated body should only involve if there is any non-compliance by either party.

Q6.c: What should be the oversight mechanism to ensure continued compliance? Please provide your comments with reasoning sharing the national / international best practices.

All Broadcaster shall have common standards and these shall be agreed by all stakeholders.

Q7: Once a new framework is established, what should be the mechanism to ensure that all CAS/ SMS comply with the specifications? Should existing and deployed CAS/ SMS systems be mandated to conform to the framework? If yes please suggest the timelines. If no, how will the level playing field and assurance of common minimum framework be achieved?

Networks that significantly deviate from the required standard should upgrade at least by implementing a cap & grow strategy. Assuming cap & grow, the time line could be rather short, as there will be no requirement for touching the existing deployment. If an incumbent system has severe security problems that cannot be fixed, a replacement incl. STB swap might be the only possible way forward.

Q8: Do you think standardization and certification of CAS and SMS will bring economic efficiency, improve quality of service and improve end- consumer experience? Kindly provide detailed comments.

In general, every operator should have natural desire for running a network with highest integrity. Weak CASes will automatically be replaced because they cut the operator's revenue. Also, content owners have an economic choice to request a minimum standard for licensing their content. So, a public standard is not required in Verimatrix' opinion.

Q9: Any other issue relevant to the present consultation.

1. Chipset – which is the integral part for implementing the security, should also support forensic watermarking going forward as this is a technology that aids in nailing the source of redistributed pirate content. This becomes more important to implement considering the market adopting IP based hybrid/Android STB's over pure linear SD & HD STB making premium content more vulnerable attacks.

2. Guidelines on IPTV clarifying medium to be multicast or unicast needs to be specified? All content houses themselves have OTT platform on unicasts with security enabled from the native DRM players in the devices/Set Top Boxes/Smart Televisions, while multicast implementation for IPTV requires a specific CAS security client as implemented in the DVB scenarios. Much clarity on this front will also enable new players & ISP's in making faster decisions in implementing a video delivery service using one of the available video security technologies complementing the network delivery mechanism . Currently there is no compliance for the Native DRMs which creates a ambiguity. Clarity from the regulator will be of immense importance.

3. Fingerprinting and Forensic watermarking services specially for IPTV (Unicast or Multicast) in addition to DVB to be provided by CAS vendor for aiding forensic investigation of any illegal redistribution of content.

4. The regulator should also consider to allow 3rd party hosted solutions for the CAS, IPTV DRM as this can help set up advanced implementation helping small and medium operators to get access to world class services at affordable costs and focus on delivering the best services to its end customers.

5. Chipsets/SoC: Security models have to be standardised and our recommendation is to move for the implementation of TEE enabled SoC's which are now available widely even in the low features chipsets. This kind of implementation is advantageous to the eco-system as the level of security is way advanced that was is being implemented today.